IN THE CLAIMS

1. (Currently Amended) A system for identifying a computer virus in responses sent in reply to a user request for content, the system comprising:

a user input device that generates a user request for content including an address of a target server and a protocol field;

a network component that executes a redirection program, the redirection program including a scan module that receives the user request for content and is capable of identifying the request as a request for content by scanning the protocol field and identifying a content-related protocol; and a proxy module that modifies the request for content by adding a redirection destination header to the request so that it is redirected to a proxy server;

a network that routes the request for content to the proxy server; and

the proxy server that receives user-defined configuration data during a negotiation phase of establishing a connection between the proxy module and proxy server, receives the request for content, removes the redirection destination header, forwards the request to the target server, and receives a response from the target server, the proxy server having a content scanning module to scan the response and a user-defined configuration data scanning module to apply user-defined configuration data to the response.

2. (Previously Presented) The system of claim 1 wherein the proxy server identifies the computer virus in the response and processes the response according to defined parameters.

3. (Previously Presented) The system of claim 2, wherein the proxy server sends at least a portion of the response to the user, the portion of the response not including the computer virus.

4. (Previously Presented) The system of claim 2, wherein the proxy server sends a notification message back to the user, the notification message containing data related to the computer virus.

5. (Original) The system of claim 1, further comprising:
a user preference module that receives user-defined parameters utilized by the proxy server when processing the response.

6. (Original) The system of claim 1, wherein the proxy module redirects the request to the proxy server by modifying the request.

7. (Original) The system of claim 6, wherein the proxy module modifies the request by adding a redirection destination header to the request.

8. (Previously Presented) The system of claim 1, wherein the proxy server further quarantines the computer virus.

9. (Previously Cancelled)

10. (Original) The system of claim 1, wherein the defined parameters are proxy server default parameters.

11. (Original) The system of claim 1, wherein the defined parameters are user-defined parameters.

12. (Original) The system of claim 1, wherein the defined parameters are a combination of user-defined parameters and proxy server default parameters.

13. (Original) The system of claim 1, wherein the scan module and the proxy module are located in a network gateway device.

14. (Original) The system of claim 5, wherein the scan module and the proxy module are located in a network gateway device.

15. (Original) The system of claim 1, wherein the network gateway device further comprises a firewall and a router.

16. (Currently Amended) A method for identifying undesirable content ~~a computer virus~~ in responses sent in reply to a user request for content, the method comprising:

receiving ,at a redirection program executing on a network computing device, input from a user computer including at least one request for content addressed to a target server, the request having an address of said target server and a protocol field;

identifying at a scan module in the redirection program the request for content by scanning the protocol field and identifying a content-related protocol;

at a proxy module in the redirection program, modifying the request by adding a redirection destination header to the request, thereby redirecting the request to a proxy server;

~~redirecting the request for content to a proxy server;~~

receiving the request for content at the proxy server;

receiving user-defined configuration data at the proxy server during a negotiation phase of establishing a connection between the proxy module and proxy server;

removing the redirection destination header from the request at the proxy server;

sending the request for content from the proxy server to the target server for generation of a response;

receiving the response from the target server at the proxy server;

decoding the response at the proxy server;

scanning the decoded response for a computer virus, junk e-mail, or pornographic content at the proxy server; ~~and~~

~~processing the response according to defined parameters~~

if a computer virus, junk e-mail, or pornographic content is detected, processing the decoded response at the proxy server according to the user-defined configuration data, re-encoding the response and appending a return address so that the response is sent to the user computer; and

if a computer virus, junk e-mail, or pornographic content is not detected, re-encoding the response and appending the return address so that the response is sent to the user computer.

17. (Currently Amended) The method of claim 16, further comprising:

identifying the ~~computer virus~~ undesirable content in the response;

modifying the response to remove the undesirable content ~~computer virus~~; and

sending the modified response from the proxy server to the user computer.

18. (Previously Cancelled)

19. (Cancelled)

20. (Cancelled)

21. (Original) The method of claim 16, wherein the request for content is redirected to the proxy server by establishing a session with the proxy server.

22. (Currently Amended) The method of claim 16, further comprising:

receiving input of at least one user-defined parameter at the proxy module which stores the parameter in a database and may forward to the proxy server during negotiation phase of the connection with the proxy server ~~for use by the proxy server in processing the computer virus~~.

23. (Original) The method of claim 22, wherein the user-defined parameter is input using a browser application.

24. (Previously Presented) The method of claim 22, wherein the user-defined parameter is sent to the proxy server by modifying the request for content.

25. (Original) The method of claim 22, wherein the user-defined parameter is sent to the proxy server during a session established with the proxy server.

26.-35. (Previously Cancelled)

36. (New) The method of claim 16 further comprising:
storing the user-defined configuration data at the proxy module.

37. (New) The method of claim 16 further comprising:
storing the user-defined configuration data at the proxy server.

38. (New) The method of claim 16 further comprising:
retrieving the previously stored user-defined configuration data at the proxy server when processing the decoded response.